ORANGE COUNTY PUBLIC SCHOOLS
Information Technology
445 W. Amelia Street Orlando, Florida 32801

Remote Use of the Network and Services via Dialup/VPN Agreement

Remote use of the Internet and automated systems (mainframe, network, or workstation-based) is not a right, but a privilege. Inappropriate use will result in cancellation of that privilege and will be reported to Employee Relations. User accounts shall be assigned or terminated at the direction of the Information Technology Department.

The person in whose name an account is issued is responsible at all times for its proper use. Persons using Orange County Schools Internet or automated systems connections must be properly authorized. They must have completed the necessary district authorization; and these must be maintained on file in the Information Technology Department. Mainframe and SAP authorizations are also kept on file in Information Technology.

Any breach in security where confidential records may have been accessed or secure information altered is a very serious problem and must be reported to the school or department administrator and the Information Technology Department immediately. This is necessary to secure systems which may be at risk and to track access records to resolve any access problem. The work location administrator will be notified of suspected access or distribution violations. It will be the responsibility of the respective administrator in collaboration with Employee Relations to follow up in investigating such reports and taking appropriate action, which may include criminal litigation. As with other district computer access, the account owner is expected to honor all guidelines in Management Directive A-9, Employee Use of Technology (see http://intranet.ocps.k12.fl.us/assets/images/directives.PDF).

Use of another individual's account (password) to remotely access the district's network is a security violation. Attempts to log on as another user will result in cancellation of privileges and notification of the responsible administrators. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to all or part of the network.

Each employee remotely accessing confidential records should be informed and acknowledge that most personally identifiable information is confidential (and, often times, directory information as well). Only those persons having direct and legitimate interest in that student or employee may view, access, or otherwise make use of such information. Those properly authorized persons are responsible for appropriate access, distribution, records security and destruction of confidential information whether "hard copy" (e.g. paper) or electronic (including mainframe SAP, server, workstation-based records; magnetic or optical disc stored records, etc.). Employees will be expected to log off properly when discontinuing remote access to the network. Employees with granted access are also expected not to let others view the information they have access to.

Non-OCPS employees will be required to request Dialup/VPN access every year. Please e-mail this request to helpdesk@ocps.k12.fl.us or fax to 407.317.3380.

Request to issue: ❒ Dialup Access ❒ VPN Access

Applicant's Name: _____ Date of Request: _____

Work Location Name: _____ Position: _____

Email Account: _____

Authorized by: _____